REMARKS:

This paper is herewith filed in response to the Examiner's Office Action mailed on May 11, 2010 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-12, 14-19, 21, 29-32, 34-35, 37-38, 40-43, 45-47, and 49-51 of the application.

More specifically, the Examiner has rejected claims 1-5, 7-9, 14, 16, 21, 29-32, 34, 37-38, 40, 42-43, 46-47, and 50-51 under 35 USC 103(a) as being unpatentable over Boyle (US6,647,259) in view of Lamb (US6,085,083), and in further of Bui (US6,412,007); rejected claims 6, 10-12, and 17-18 under 35 USC 103(a) as being unpatentable over the combination of Boyle and Lamb, in view of Bui, and further in view of Chavez (US6,591,102); rejected claims 15, 35, 41, 45, and 49 under 35 USC 103(a) as being unpatentable over the combination of Boyle in view of Bui, and further in view of Basilier (US6,412,007); and rejected claim 19 under 35 USC 103(a) as being unpatentable over the combination of Boyle and Lamb, in view of Bui, and further in view of Wright (US6,957,061). The Applicant respectfully traverses the rejection.

Claims 1, 3-11, 17-19, 21, 29-32, 38, 42, 46, and 50-51 have been amended. Claims 14-16 have been cancelled. Support for the amendments can be found on page 12, line 23 to page 15, line 27 and page 18, lines 23-27 of the Application as filed. No new matter is added.

Rejection of the independent claims under 35 USC 103(a)

Although the Applicant does not expressly or impliedly agree with the rejections, the Applicant submits that in order to facilitate the prosecution of this patent application towards allowance each of the independent claims 1, 7, 21, 29-31, 42, 46 and 50-51 have been amended in a somewhat similar fashion. For example, claim 1 now recites in part that:

> A method, comprising: in response to a request by a user to initiate a session for a service with a communication system, receiving from the communication system, at an authentication and authorization device in a home network of the user, a

> request for an authorization and authentication of the user to initiate the session; and in response to the request for the authorization and authentication of the user, sending by the authentication and authorization device, to a server node in the communication network, information comprising an authorization and authentication profile associated with the user, wherein the authorization and authentication profile contains information which allows the server node to directly authorize and authenticate the user, without contacting the authentication and authorization device, in order to initiate a subsequent session for a service with the communication system for the user, and wherein the authorization and authentication profile further contains information defining that the authentication and authorization device is to be contacted when at least one condition is met, where the at least one condition comprises that a number of simultaneous sessions for the user is equal to a predetermined number.

The Applicant notes that the amendments are supported at least on page 12, line 23 to page 15, line 27 and page 18, lines 23-27 of the Application as filed. The Applicant submits that claim 1 is patentably distinguishable from the references cited.

Boyle

In the rejection of claim 1 the Examiner states:

> "Consider claim 1, Boyle et al. clearly show and disclose a method, comprising: using an authorization and authentication profile associated with a user (HLR record for mobile unit [col. 3 lines 23-26]), including the authorization and authentication profile is sent from an authentication and authorization device located in a home network to a server node (home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system [col. 3 lines 46-501); and the authorization and authentication profile is stored at the server node (sends a profile of the mobile user to the visited wireless system; profile is obtained from the HLR record [col. 3 lines 46-50])," (see page 3 of the Office Action).

The Applicant submits that the language of claim 1, to which Boyle has been asserted against, now recites:

> "in response to a request by a user to initiate a session for a service with a communication system, receiving from the communication system, at an

> authentication and authorization device in a home network of the user, a request for an authorization and authentication of the user to initiate the session; and in response to the request for the authorization and authentication of the user, sending by the authentication and authorization device, to a server node in the communication network, information comprising an authorization and authentication profile associated with the user."

The Applicant submits that Boyle relates to method for limiting the number of simultaneous call forwarding attempts when a mobile unit responds to a call request. In Boyle, the mobile unit will register with a home wireless system. Then after receiving the registration from a mobile unit the home wireless system sends a profile of the mobile user to a visited wireless system (col. 3, lines 41-49). Further, according to Boyle:

> "The HLR record for mobile unit 102 preferably includes a field that indicates the number of simultaneous call forwarding requests that are permitted for mobile unit 102," (col. 3, lines 23-26); and
>
> "It should be understood that for each of the ladder diagrams in FIGS. 2-5, the mobile unit will register with the home wireless system. The home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system," (col. 3, lines 45-48); and
>
> "The profile is typically obtained from the HLR record for the mobile user, and includes the origination major class for the mobile unit, the terminating major class for the mobile unit, the call forwarding capabilities of the mobile unit, as well as other features associated with the mobile unit," (col. 3, lines 49-54).

First, the Applicant submits that Boyle does not disclose or suggest operations that relate to a request for an authorization and authentication of a user. The Applicant submits that the home wireless system of Boyle is neither receiving a request for an authorization and authentication nor responding to a request for authorization and authentication of a mobile unit in Boyle, as appears asserted in the rejection. Boyle merely discloses a method to notify a visited wireless system of information including the call forwarding capabilities of the mobile unit.

Further, the Applicant submits that the information including the call forwarding capabilities of the mobile unit in Boyle is not used for any operation related to authorization and authentication

of the mobile unit. In addition, the Applicant submits that there appears to be nothing in Boyle which elaborates on whether the information including the call forwarding capabilities, that is sent to the visited wireless system of Boyle, is even used by the visited wireless system in Boyle. The Applicant submits that Boyle merely states that the "Host wireless system 103 also determines the threshold number of simultaneous call forwarding attempts that are allowed for mobile unit 102. This is preferably done by retrieving a value that is stored at host wireless system 103," (emphasis added), (col. 4, lines 32-37). However, in any case, the Applicant submits that Boyle does not disclose or suggest that the information sent to, or retrieved by, the visited wireless system of Boyle is somehow related to an authorization and authentication operation as asserted in the rejection.

The Applicant submits that, for at least these reasons, Boyle does not disclose or suggest at least where claim 1 recites in part:

> "in response to a request by a user to initiate a session for a service with a communication system, receiving from the communication system, at an authentication and authorization device in a home network of the user, a request for an authorization and authentication of the user to initiate the session; and in response to the request for the authorization and authentication of the user, sending by the authentication and authorization device, to a server node in the communication network, information comprising an authorization and authentication profile associated with the user"

The Applicant submits that, for at least these reason the references cited do not disclose or suggest claim 1.

The Applicant notes that in the rejection the Examiner states:

> "However, Boyle et al. fail to specifically disclose that the profile allows the server node to authorize and authenticate directly," (see page 3 of the Office action).

The Examiner then cites Lamb in order to allegedly overcome this admitted shortfall of Boyle.

Lamb

In the rejection the Examiner states:

> "Lamb clearly shows and discloses wherein the authorization and authentication profile contains information which allows the server node to authorize and authenticate the user directly without contacting the authentication and authorization device (each MSC communicating to an HLR has a corresponding MPCM file record in the MPCM file of the HLR; SUBS file **222** is the "subscribers' files" which store subscribers' profiles on a per subscriber basis; FRAUD-INFO segment of a subscriber's profile record indicates whether or not fraud protection (i.e., FP check) is authorized for this subscriber; The OPT7_IND field indicates whether the Visitor Location Register (VLR) serving this MSC can perform an authentication (AC) check [col. 2 line 61- col. 3 line 6, col. 4 lines 29-col. 5 line 10, lines 46-50)," (emphasis added), (see page 3 of the Office action).

The Applicant submits that the rejection is unclear. In the rejection the Examiner appears to assert that the MPCM file record, the subscriber files, the FRAUD-INFO segment, and the OPT7_IND field of Lamb somehow disclose or suggest a profile which allows a server node to authorize and authenticate a user directly. The Applicant disagrees.

The Applicant submits that according to Lamb if an unlocked phone becomes inactive for a predetermined amount of time the home location register (HLR) invokes a fraud protection feature until the subscriber unlocks the phone with feature code and PIN entries (col. 3, lines 2-6). Further, Lamb discloses that an "AC 146 authenticates a subscriber's cellular phone through the use of an encrypted number called the A-Key," (emphasis added), (col. 2, line 32-34).

First, the Applicant submits that Lamb clearly does not disclose or suggest at least where claim 1 now recites:

> "wherein the authorization and authentication profile contains information which allows the server node to directly authorize and authenticate the user, without contacting the authentication and authorization device, in order to initiate a subsequent session for a service with the communication system for the user"

The Applicant submits that neither the indication of fraud protection feature nor the

authentication check of Lamb relate to information which allows a server node to directly authorize and authenticate the user in order to initiate a subsequent session for a service with the communication system for the user without contacting the authentication and authorization device in a home network of the user. Rather, the Applicant submits that Lamb relates to alternative methods to unlock a phone.

Lamb discloses:

> "Alternatively, a cellular carrier may bypass the FP check in areas that support AC processing to provide convenience to the subscribers so that they do not have to enter their PINs to use their cellular phones," (emphasis added), (col. 6, lines 43-46); and
>
> "Then the mediation module refers to the AC/FP lookup table in HLR 636 to determine whether an AC check, an FP check, or both should be performed on the subscriber's cellular phone. After having determined the appropriate check or checks that are needed, the mediation module sends an appropriate request to the conventional components of HLR 636 to perform the check or checks on the subscriber's cellular phone," (emphasis added), (col. 7, lines 32-39).

The Applicant submits that Lamb, as stated above, indicates that the cellular carrier may bypass a fraud protection check in areas that support an authentication check. However, the Applicant submits that Lamb is unclear with regards to the authentication check (AC). The Applicant again submits that Lamb simply states that the "AC 146 authenticates a subscriber's cellular phone through the use of an encrypted number called the A-Key," (emphasis added), (col. 2, line 32-34). The Applicant contends that the AC processing in Lamb relates to an alternative to a fraud protection feature of a cellular phone, where the authentication check somehow unlocks the phone so that the subscribers do not have to enter their PINs to use their cellular phones.

Further, the Applicant re-submits that, for at least these reasons, Lamb does not relate to sending information to a server node which allows the server node to directly authorize and authenticate the user in order to initiate a subsequent session for a service with the communication system for the user without contacting the authentication and authorization device.

In the Office Action the Examiner states:

> "However, Boyle et al., as modified by Lamb, fail to specifically disclose authorization is verified when the number of simultaneous session is equal to a predetermined number," (see page 4 of the Office Action).

The Examiner then applies Bui in order to allegedly overcome the admitted shortfalls.

Bui

In the rejection the Examiner states:

> "In the same field of endeavor, Bui et al. clearly show and disclose wherein the authorization and authentication profile further contains information defining that the authentication and authorization device is to be contacted when a number of simultaneous sessions for the user is equal to a predetermined number (after determining the number of sessions that are currently established for a particular entity, the local DSC compares the number to a session threshold value, wherein the threshold identifies the maximum number of session allowed before SLOW LANE authorization is required; each DSC maintains its own local copy of the information maintained in the global database [fig. 2, col. 5 lines 36-50, line 60-col. 6 line 8, lines 12-22, col. 18 lines 45-53])," (see page 4 of the Office Action).

It is noted that, in Bui, a session threshold value is assigned to entities and one or more of the entities are associated with a particular user. The entities associated with the user are also assigned to an authoritative DSC. (col. 23, lines 2-9). As cited by the Examiner, Bui discloses that when a client sends a request to a network access server requesting that a connection be established for accessing a network system, the network access server then sends an authorization request message to a local DSC (col. 5, lines 36-42). The local DSC then determines whether a number of established sessions exceed a local threshold value that identifies a maximum number of sessions that may be established for a particular entity. If the established sessions exceed this value the local DSC cannot authorize the connection request and the local DSC must send an additional authorization request to the authoritative DSC (col. 6, lines 12-25).

The Applicant submits that Bui does not disclose or suggest at least where claim 1 relates to

information received from an authentication and authorization device in a home network of a user defining that the authentication and authorization device is to be contacted when at least one condition is met, where the at least one condition comprises that a number of simultaneous sessions for the user is equal to a predetermined number. Rather, the Applicant submits that there is nothing in Bui to indicate that a number of simultaneous sessions for the user is provided in information received from an authentication and authorization device in a home network of a user. The Applicant submits that Bui does not disclose or suggest that the authoritative DCS or the local DCS of Bui is in a home network of a user. Moreover, the Applicant can not find that the threshold value in Bui is even received in response to a request for an authorization and authentication of a user to initiate a service. Rather, according to Bui the DSC retrieves the threshold value which is maintained at the entity and adjusted for performance of the distributed system in Bui (col. 5, line 56 to col. 6, line 7).

The Applicant submits that, for at least these reasons, Bui does not disclose or suggest at least where claim 1 recites in part:

> "wherein the authorization and authentication profile further contains information defining that the authentication and authorization device is to be contacted when at least one condition is met, where the at least one condition comprises that a number of simultaneous sessions for the user is equal to a predetermined number"

Further, the Applicant submits that none of the references cited overcome at least the above stated shortfalls of Boyle, Lamb, and Bui.

The Applicant contends that, for at least the reasons stated, even if the references were combined, which is not agreed to as proper, the combination would still fail to disclose or suggest claim 1. Thus, the rejection of claim 1 is seen to be improper and the rejection should be removed.

In addition, the Applicant submits that, for similar reasons, the foregoing amendments to the independent claims 7, 21, 29, 30, 31, 42, 46, 50, and 51 also place these claims in condition for allowance in view of the references cited. Therefore the Examiner is requested to remove the

rejections and allow these claims.

In addition, the Applicant submits that none of the references cited disclose or suggest at least where dependent claim 4 recites in part "wherein the at least one condition further comprises that if a subsequent session is a multimedia session then the authentication and authorization device is to be contacted." Therefore, the Examiner is requested to remove the rejection and allow claim 4.

In addition, for at least the reason that dependent claim 17 recites features similar to claim 4, the references cited do not disclose or suggest claim 17 and claim 17 should be allowed.

Further, the Applicant notes the claim 6 depends from claim 4. The Applicant submits that none of the references cited disclose or suggest at least where claim 6 recites in part "wherein the at least one condition further comprises that if a session is initiated at a predefined time of day and the user is being served by at least one of a plurality of predetermined networks then the authentication and authorization device is to be contacted." Thus, the Applicant requests that the Examiner remove the rejection and allow claim 6.

Additionally, for at least the reason that dependent claim 18 recites features similar to claim 6, the references cited do not disclose or suggest claim 18 and this claim should be allowed.

Furthermore, as the claims 2-6, claims 8-12 and 17-19, claims 32 and 34-35, claims 37-38 and 40, claims 43 and 45, and claims 47 and 49 depend from claims 1, 7, 30, 31, 42, and 46, respectively, the rejections of these claims is improper, and all the claims 1-12, 17-19, 21-27, 29-32, 34-35, 37-38, 40-43, 45-47, and 49-51 should be allowed.

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1-12, 17-19, 21-26, 29-32, 34-35, 37-38, 40-43, 45-47, and 49-51. The Examiner is respectfully requested to reconsider and remove the rejections of and to allow all of the pending as now presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted:

9/13/2010

John A. Garrity — Date

Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH ATTORNEYS AT LAW, LLC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

9/13/2010 — Date

Claire F. Brian — Name of Person Making Deposit